Altiris™ Patch Management Solution for Windows® 7.1 SP1 from Symantec™ Release Notes

Symantec™

Altiris™ Patch Management Solution for Windows® 7.1 SP1 from Symantec™ Release Notes

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Altiris™ Patch Management Solution for Windows® 7.1 SP1 from Symantec™ Release Notes

This document includes the following topics:

- About Altiris Patch Management Solution for Windows
- What's new in Patch Management Solution for Windows 7.1 SP1
- Software that Patch Management Solution for Windows supports
- General installation and upgrade information
- About upgrading Patch Management Solution for Windows
- System requirements
- Platforms supported by Patch Management Solution for Windows
- Known issues
- Fixed issues
- Other things to know
- Documentation that is installed
- Other information

About Altiris Patch Management Solution for Windows

Altiris Patch Management Solution for Windows from Symantec lets you scan computers for required software updates, report on the findings, and automate the downloading and distribution of required updates for Windows software. You can review and download specific patches from vendors such as Microsoft, Adobe, Java, Sun Microsystems, and many others. You can then apply patches to the computers that need them.

Patch Management Solution for Windows is a component of Patch Management Solution. When you install Patch Management Solution using Symantec Installation Manager, the following components are installed:

- Patch Management Solution for Windows
- Patch Management Solution for Linux
- Patch Management Solution for Mac

Patch Management Solution is part of the following suites:

- Altiris Client Management Suite from Symantec
- Altiris Server Management Suite from Symantec
- Altiris IT Management Suite from Symantec

What's new in Patch Management Solution for Windows 7.1 SP1

In the 7.1 SP1 release of Patch Management Solution for Windows, the following new features are introduced:

- Greater coverage of third-party software that can be scanned for vulnerabilities and patched.
  See "Software that Patch Management Solution for Windows supports" on page 5.
- Ability to roll out service packs for Microsoft products.
- Ability to replicate a critical software update policy to child Notification Server computers immediately.
- You do not have to stage software bulletins before you can distribute them. Software updates can be downloaded when you run the **Distribute Software Updates** wizard.
- Software Update Plug-in now supports Service Pack 1 of Windows 2008, 2008 R2, and 7.

- Reliability and performance improvements.

Software that Patch Management Solution for Windows supports

Patch Management Solution for Windows lets you install software updates for software from the following vendors:

- 7-Zip
- Adobe Systems
- AOL
- Apple
- Citrix Systems
- Foxit Corporation
- Google
- Hewlett-Packard
- Microsoft
- Mozilla
- Nullsoft
- Opera Software
- Oracle
- RealNetworks
- RealVNC
- Research In Motion
- Skype Technologies S.A.
- Sun Microsystems
- WinZip

General installation and upgrade information

You install this product by using Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

For more information, see the *IT Management Suite Implementation Guide* at http://www.symantec.com/docs/DOC3464.

For general information about migrating Symantec Management Platform and suites to 7.1 SP1, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.1 SP1* at http://www.symantec.com/docs/DOC3988
- *IT Management Suite Migration Guide version 7.0 to 7.1 SP1* at http://www.symantec.com/docs/DOC3989

For additional information about upgrading to Patch Management Solution for Windows SP1, see About upgrading Patch Management Solution for Windows

About upgrading Patch Management Solution for Windows

You upgrade this product from 7.1 to 7.1 SP1 by using the Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

Software update packages, software update policies, and downloaded software updates metadata from previous versions of Patch Management Solution for Windows are not compatible with 7.1 SP1. After you upgrade to 7.1 SP1, you must run the clean-up task that removes incompatible data. A link to the clean-up task is available on the **Import Patch Data for Windows** page.

For general information about migrating Symantec Management Platform and Patch Management Solution for Windows from 6.x and 7.0, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.1 SP1* at: http://www.symantec.com/docs/DOC3988
- *IT Management Suite Migration Guide version 7.0 to 7.1 SP1* at: http://www.symantec.com/docs/DOC3989

After you migrate or upgrade the solution, you must upgrade the Symantec Management Agent and the software update plug-in that are installed on the managed computers.

For more information about upgrading the Symantec Management Agent, see *Symantec Management Platform Help*.

System requirements

Patch Management Solution for Windows requires the following:

- Symantec Management Platform 7.1 SP1

Platforms supported by Patch Management Solution for Windows

The Patch Management Solution for Windows component of Patch Management Solution supports the following operating systems:

- Windows XP SP2 and later, 32-bit and 64-bit
- Windows Vista SP1 and later, 32-bit and 64-bit
- Windows 7, including SP1, 32-bit, and 64-bit
- Windows Server 2003 SP2 and later, 2003 R2 SP2 and later, 32-bit and 64-bit
- Windows Server 2008 32-bit and 64-bit, 2008 Core, 2008 R2, 2008 R2 Core, including SP1
- Windows Hyper-V Server 2008
- Windows XP Embedded SP3
  For the Software Update Plug-in to work properly on Windows XP Embedded SP3, the following software must be installed on the client computer:
  - Windows Installer Service
  - TCP/IP Networking with File Sharing and Client for MS Networks
  - TCP/IP Networking
  - Secondary Logon Component
    This component is required to use the "Run with right as" setting on Notification Server side.
  - Copy and Compare Tools
    Some custom action updates require the xcopy.exe tool to be installed.

Known issues

The following are known issues for this release. If additional information about an issue is available, the issue has a corresponding Article link.

For the most up-to-date information, latest workarounds, and other technical support information about this solution, see the Technical Support knowledge base.

The known issues are separated into the following groups:

- Installation and upgrade issues
  See Table 1-1 on page 8.
- Hierarchy and replication issues
  See Table 1-2 on page 10.
- Software updates installation issues
  See Table 1-3 on page 13.
- Other known issues
  See Table 1-4 on page 17.

Table 1-1 Installation and upgrade issues

Issue	Description	Article link
After upgrade, change the **Software Update Package Location** setting.	Software update packages from previous versions of the product cannot be used by Patch Management Solution for Windows 7.1 SP1. If you specified a UNC path for the **Software Update Package Location** setting, do one of the following after the upgrade: ■ Delete all of the packages at the UNC location. Use this option if there are no other Notification Server computers that may need the packages and you do not use Patch Management Solution for Linux. ■ Specify a different UNC path as the new location for storing the packages. Use this option if other Notification Server computers are still using this path.	
An issue when breaking the hierarchy before migrating to 7.1 SP1.	You must break the hierarchy if you are performing a migration from 7.0 to 7.1 SP1. After you break the hierarchy on the parent Notification Server computer, sometimes the child Notification Server computer retains its association with the parent server. Workaround: Also break the hierarchy on the child Notification Server computer.	
The **Download from staging location** setting is reset to default.	The **Download from staging location** setting on the **Core Services** page is reset to default after upgrade.	

Table 1-1 Installation and upgrade issues *(continued)*

Issue	Description	Article link
License count is reset after upgrade.	The count of licenses in use is reset after you upgrade to 7.1 SP1. The count will increase after you upgrade the Software Update Plug-in on the client computers to version 7.1 SP1, and then run the system assessment scan.	
SQL queries in automation policies are overwritten.	The query parameters in the automation policies (**Item Status Changed After PM Import**, **Maintain Retired Machine Historical data**, **Software Update Advertisement Disabled**, **Software Update Policy Failed**) are not migrated during an upgrade from 7.x to this version of Patch Management Solution. Parameters in the default automation policies can be migrated, but SQL queries are overwritten. Symantec recommends that if you want to customize an automation policy, you clone the policy, and then make changes to the clone.	
Sometimes **Inventory Interval** in **Windows Vulnerability Analysis Policy** cannot be migrated.	If the **Inventory Interval** value was set to 24 hours or longer, it cannot be converted to a schedule. In this case, the default schedule is used (every 4 hours every day).	
Old server name is displayed in the **Compliance summary** report after the upgrade.	After the upgrade, the old Notification Server computer's name is displayed in the **Compliance summary** report.	
Non-inherited permissions are not migrated from 6.x to 7.x.	Non-inherited permissions for security roles are not migrated from 6.x to 7.x.	
Cloned Software Update Agent Policies are not visible after upgrade.	Cloned Software Update Agent policies that were located at **Settings > Agents/Plug-ins > Software > Windows Software Update Agent > Settings** are not visible in the console after you perform an upgrade from 7.x to 7.1 SP1. To resolve this issue, use the search option in the console to find missing configuration policies. After they have been found, right-click them and select move. They can now be moved to the location in which the default policy is located. If the name of the policy is unknown, the following query can be run on the SQL Server to obtain the names: `SELECT Guid, [Name] FROM vItem WHERE ClassGuid = '5e5bde22-c290-4a94-a36c-c5076da6d565' AND Attributes & 256 = 0`	TECH45206

Table 1-2 Hierarchy and replication issues

Issue	Description	Article link
Only two-level hierarchy is supported.	Although Symantec Management Platform lets you create multi-level hierarchies, Patch Management Solution supports only two-level hierarchy. A child Notification Server computer cannot be a parent to another Notification Server computer.	HOWTO44217
An issue with default replication schedules.	There can be issues with data replication if all three replication rules (Windows, Novell, and Red Hat) run at the same time, which is 11:00PM by default. Symantec recommends that you stagger the replication schedules or disable replication for the vendors that you do not use.	
Scheduled client tasks are not replicated to the child immediately.	When you create a schedule for a client task (for example, **Run System Assessment Scan on Windows Computers**), and include managed computers from a child into the target, the schedule does not replicate to the child Notification Server computers immediately. Workaround: Use the **Run now** option.	

Table 1-2 Hierarchy and replication issues *(continued)*

Issue	Description	Article link
Excluded software channels are not replicated to the child when included again.	An issue occurs with the **Import Patch Data for Windows** task in the following scenario: 1 You check a software channel (for example, Adobe), run, and then replicate the task. 2 You uncheck the software channel, but do not select the **Delete data for excluded software products** option. Then you run and replicate the task. 3 You check the software channel, run, and then replicate the task. As a result, the software channel does not become enabled on the child Notification Server computer. To prevent this issue from happening, in a hierarchy environment, always select the **Delete data for excluded software products** option. If this issue already occurred, do the following on the parent Notification Server computer: 1 Check this option. 2 Uncheck all vendors. 3 Run the task. 4 Replicate the task. 5 Check the vendors that you want to import. 6 Run the task. 7 Replicate the task.	
Exporting software update policies from parent to child is not supported.	Do not attempt to export a software update policy on the parent Notification Server computer and import it on the child. Instead, use the built-in replication functionality.	
An issue with the **Allow Package Server Distribution with Manual Prestaging** setting.	The **Allow Package Server Distribution with Manual Prestaging** settings are replicated, but displayed incorrectly in the Symantec Management Console of the child Notification Server computer. The functionality is not affected, you can ignore this user interface issue.	

Table 1-2 Hierarchy and replication issues *(continued)*

Issue	Description	Article link
Reports do not display any data from hierarchy.	With the exception of the **Compliance Summary** report, Patch Management Solution reports do not display any data from the child Notification Server computers. Only the data for the current Notification Server computer is displayed in patch reports. There is a known issue with some of the **Compliance Dashboard** web parts that may include data from the child Notification Server computers. You can drill down or view the **Compliance > Compliance Summary** report for more accurate data.	
The **Check Software Update Package Integrity Task** cannot be run on the child.	The **New schedule** button on the **Check Software Update Package Integrity Task** page is disabled on the child Notification Server computer. Workaround: Schedule the task on the parent Notification Server computer. Then edit the schedule on the child.	
Replicating data between different versions of Patch Management Solution is not supported.	Although some items may replicate between different versions of Patch Management Solution that are installed on parent and child Notification Server computers, Symantec does not recommend doing this. If you want to use hierarchy and replication, Patch Management Solution versions must be the same on the parent and child.	
Errors occur when the plug-in requests configuration for replicated software update tasks before the associated packages have been re-created.	During software update policy replication, the policies are created before the packages have been downloaded to the child Notification Server computers. If a software update plug-in requests configuration during this time, errors appear in logs as the policies are incomplete until the packages are downloaded. After the packages are downloaded, the errors will no longer occur.	
Notification Server Item replication deletes any task history on the child.	Replication of items down a hierarchy deletes any task history on the child for the Patch Management server tasks.	
Differential replication mode does not replicate bulletin data to the child computer that has a new language.	In a hierarchy, the bulletin data is not replicated to the child Notification Server computer if all the following criteria are true: ■ You add a new language to the child server. ■ The bulletins on the parent Notification Server computer have not changed. ■ The replication is run in Differential mode.	

Table 1-3 Software updates installation issues

Issue	Description	Article link
The language of some applications cannot be detected.	At the moment, Patch Management Solution for Windows can detect the language of the following applications: Microsoft SQL Server 2000, 2005, 2008, Microsoft Office 2003, 2007, 2010. The language of other applications cannot be detected. In this case the language of the operating system is used and updates for this language are installed. This may result in applications changing their language to the language of the operating system after the update.	
Installation of some updates cannot be performed silently.	Some updates do not support silent installation. Some dialog or progress windows may be visible to the user of the managed computer. This issue does not affect the installation, and can be ignored.	
Some software cannot be updated when System Account is used.	Installation of some updates is possible only under a logged-in or a specified user. Use the **Run with rights** setting to configure the user. The issue is known to occur under the following conditions: ■ When installing x86 Java updates on 64-bit operating systems ■ When upgrading Opera 9 software	
Installation of MS05-035 and MS06-003 fails.	Installation of Microsoft updates MS05-035 - Q895333 and MS06-003 - Q892842 may fail. Workaround: Install update MSWU-022 before installing these updates.	
An installation prerequisite is required for MSWU-232.	Before you install MSWU-232, make sure the following updates are installed: ■ MSWU-231 for Windows 2003 SP1, 32-bit and 64-bit; Windows XP SP2 32-bit, XP SP1 64-bit ■ MSWU-109 for Windows Vista Gold, 32-bit and 64-bit	
MS07-047 cannot be installed on Windows 2003.	MS07-047 (WindowsMedia10-KB936782-x86-ENU.exe) does not install on Windows 2003.	

Table 1-3 Software updates installation issues *(continued)*

Issue	Description	Article link
Installation of some software updates may fail.	Some updates may fail to install in certain conditions. The following updates are known to have issues: ■ Flash Player All Mozilla Firefox browser windows and all instances of Flash Player must be closed before installation. Symantec recommends that you update Flash Player 7.x, 8.x, and 9.x to the latest version. ■ Real Player Installation may fail if a limited user is logged in to the system. ■ Mozilla Firefox version 1.5, 2.0 and 3.0 All Mozilla Firefox browser windows must be closed before installation. ■ Opera Silent installation may fail on Windows XP. ■ Adobe Reader version 7 and 8 All instances of Adobe Reader, including those opened inside of a browser, must be closed before installing updates. Symantec recommends that you install Adobe Reader updates shortly after a computer restart. ■ ISA Server 2000 Security Patch for Web Proxy Service and H.323 ASN DLL (MS01-045) Installation of this hot fix requires user interaction on the target computer. The user must click **Yes** in the installation dialog box. Additional information about update installation prerequisites may be available in the Resource Manager or on the vendor's Web site. Also, see the HOWTO article for details.	HOWTO54657
SWUN-001 is an uninstaller.	The bulletin SWUN-001 (sw_uninstaller.exe) is always displayed as missing for every computer with Shockwave 7, 8, and 10. This is an uninstaller that can be used to uninstall Shockwave player for remediation.	
Only system-level installation of Google Chrome can be patched.	Patch Management Solution for Windows can patch only system-level (installed for all users) installation of Google Chrome. Patching user-level installations is not supported.	

Table 1-3 Software updates installation issues *(continued)*

Issue	Description	Article link
Some vendors provide only the latest versions of software updates for download.	For some software, only the latest version of software updates is available for download from the vendor's Web site. On the **Remediation Center** page, you may see that a bulletin contains version A, but when you start downloading the update, version B is downloaded instead. If you already downloaded software update version A and created software update policies, a copy of the software update file version A is kept on the Notification Server computer. In this case, you can distribute update A until you decide to delete or redownload the package. At this time Google Chrome is known to have this issue.	
Some software updates are shown as not installed in the **Windows Update** dialog box.	Some software updates that you install using Patch Management Solution can be shown as not installed on the managed computers, in the **Windows Update** dialog box. This issue occurs because the executable is a full software release, not a patch. Symantec recommends that you use Altiris Software Management Solution from Symantec to roll out this software. The following software updates are known to have this issue: ■ KB982671 - Microsoft .NET Framework 4 ■ KB968930 - Windows PowerShell 2.0 and WinRM 2.0 ■ KB940157 - Windows Search 4.0 IE8 - Internet Explorer 8 ■ KB2526954 - Microsoft Silverlight IE9 - Internet Explorer 9 ■ KB2463332 - Windows Internal Database Service Pack 4	
Some software updates are not detected as applicable.	Some software updates are not detected as applicable, although they are shown as needed in the **Windows Update** dialog box. The following bulletins are known to have this problem: KB978542, KB2345886, KB976382, KB970430, KB975929, KB980248, KB937286, KB951847, KB967642 You can use other means of delivering these software updates, for example use Altiris Software Management Solution from Symantec.	
Chinese (Hong Kong S.A.R.) is not supported.	Patch Management Solution for Windows does not support Chinese (Hong Kong S.A.R.). Only Chinese Simplified and Chinese Traditional are supported.	

Table 1-3 Software updates installation issues *(continued)*

Issue	Description	Article link
Some updates require original installation media.	Some updates may require original installation media. The updates that are known to require one are as follows: ■ Microsoft Project 2003 SP3 ■ Microsoft Visio 2003 SP3 ■ Citrix Presentation Server If the product was installed from a CD/DVD, then the original CD/DVD must be inserted in the disk reader on the client computer. If the product was installed from a network location, then anonymous access from the client computer to this location must be available to install the update.	

An issue occurs when installing Sun-Java updates.	When Java software is in use on the client computer, the update cannot be installed silently. A "Close applications" dialog box appears on the client that prevents the update process from proceeding.
	Workaround: You can add a 'tskill java /A' command into the installation script to terminate the Java processes:
	`...`
	`"cmd.exe" /C start /wait NET STOP "JAVA QUICK STARTER"`
	`tskill java /A`
	`"cmd.exe" /C start /wait %LSFN% /s "IEXPLORER=1 MOZILLA=1" /quiet /norestart`
	`"cmd.exe" /C start /wait NET START "JAVA QUICK STARTER"`
	`...`	

When a maintenance window is configured, the update installation does not run on the schedule.	If a maintenance window opens before the software update installation schedule, the schedule (including the **Start/End dates**) is disregarded and the software update gets installed before the scheduled time. This issue occurs when **Override Maintenance Windows settings** is not checked.	
Microsoft Office components must be on the same Service Pack level.	Issues occur when various Microsoft Office components are having different Service Pack versions applied.	

Table 1-4 Other known issues

Issue	Description	Article link
An issue when using FTP as patch data alternative download location.	If you want to use an FTP location as the alternative download location on the **Import Patch Data** page, on the Notification Server computer, add the C:\Program Files\Altiris\Notification Server\Bin\AeXsvc.exe service to the firewall exception list.	
Relocating packages from an UNC location to another location does not work.	If on the **Core Services** page you change the **To Location** value from an UNC path to another path, the packages will not be relocated. Workaround: Relocate the packages manually.	
An issue occurs when accessing the AexPatchUtil.exe utility.	A non-administrator cannot navigate to the AexPatchUtil.exe utility using the command prompt because of access restrictions to the C:\Program Files\Altiris folder. This issue occurs only on the Notification Server computer. Workaround: `cd` straight to the C:\Program Files\Altiris\Altiris Agent\Agents directory.	
Software updates cannot be downloaded from an alternate download location on a non-IIS package server.	Only UNC paths can be used as an alternate download location on a non-IIS Windows package server. If you specify a local path on the server as the alternate download location, the software updates are not downloaded from a package server that does not have IIS installed.	
Sometimes policy schedules work incorrectly across timezones.	Sometimes, when you create a schedule for a policy and select either **Use Agent time** or **Use Server time**, the policy does not run as planned on the endpoints that are located in a different time zone. Workaround: Use the **Coordinate using UTC** option.	
The **Use application credentials** option does not work.	The **Use application credentials** option on the **Import Patch Data for Windows** page does not work. Workaround: Click **Use these credentials** and type application or other credentials.	
An issue with re-imaged endpoints.	An issue occurs when you re-image or reinstall an operating system on an endpoint. Software update plug-in is not able to process the policies and install software updates. Workaround: Restart the Symantec Management Agent service or restart the computer.	
Patching of software that is installed into a virtual layer is not supported.	Patches that you apply to the software in a virtual layer might not be applied correctly and can corrupt the system.	

Table 1-4 Other known issues *(continued)*

Issue	Description	Article link
Packages are not always downloaded to managed computers at the correct time.	Occasionally, software update packages may not be downloaded immediately to managed computers. This is due to a timing issue where the initial download is not triggered by Software Management and the status of the package is not updated. The packages will be downloaded when the update install schedule fires or when the next maintenance window opens.	
When you click **Save Changes** in a policy, a confirmation message displays "Saved Changes" even though the policy is still being saved.	When you edit a Software Update policy, the screen is updated with the text "Saved Changes" even though the task that saves the changes made to the policy and underlying advertisements may still be running. If the changes that you made do not appear on the screen immediately, refresh the screen after a few seconds. Your changes should appear after the refresh.	
The Software Update Plug-in stays in the "Update Pending" state after the dialog box closes.	Occasionally, clicking **Install Now** on the **Software Update Installation** dialog box or waiting for the dialog box to close itself does not result in the immediate installation of a software update. The installation starts five minutes after the dialog box has closed, when the Software Update Plug-in wakes up and checks its state.	
Incorrect data is displayed in the update delivery summary Web part.	Sometimes, the data that is displayed in the **Microsoft Software Update Delivery Summary** Web part on the patch management home page does not match the data that is displayed in the drill-down report.	
Sometimes policies with a custom schedule can trigger other policies.	When you set a custom installation schedule for a policy, other policies with a default schedule can also be triggered on the client computers and software updates will be installed. Other policies that have a custom schedule set are not affected by this issue. They will run at their scheduled time.	
The **Software Bulletin Details** report shows the computers that are out of the scope of the current console user.	In the **Software Bulletin Details** report, in the **Applies To** column, the number of all applicable computers is shown, including those for which the current console user has access and those for which access is disabled.	
Update installations that require a computer restart are shown as complete.	The **Windows Software Update Delivery Summary** report shows update installations that require computer restart as complete. You can use the **Restart Status** report to view if any computers are pending restart.	

Fixed issues

The following are the previous issues that were fixed in this release. If additional information about an issue is available, the issue has a corresponding Article link.

Table 1-5 Fixed issues

Issue	Description	Article link
Incorrect numbers can be displayed in compliance reports.	In a rare case, when more than one update in a bulletin is applicable to the same computer, the **Applicable**, **Installed**, and **Vulnerable** columns can display incorrect data.	
Issue with package migration on non-default installation of the 7.1 server.	Migration Wizard copies the software update packages to the same location as the one that was used on the old 7.0 server. If you installed Symantec Management Platform 7.1 to a location that is different from 7.0, you must then move the packages manually to the new location, that is specified on the Core Services page.	
Incorrect count of computers with software update plug-in is displayed on the portal page.	After you break up the hierarchy and upgrade Patch Management Solution from 7.0 to 7.1, the count of computers with software update plug-in in the **Microsoft Configuration Summary** Web part may be incorrect. The drill-down displays the correct number of computers.	
Download QChain settings are not migrated after upgrade from 7.x.	Some settings on the **Download QChain** page are reset to default after the upgrade.	
Some settings cannot be locked from editing on a child.	The parent Notification Server administrator cannot lock the **Scan Interval** and **Report Results** settings on the **Adobe/Microsoft Vulnerability Analysis** pages from being edited on a child.	
Software advertisements are removed from software update policies.	This issue can occur when software update policies are being replicated down a hierarchy from a parent to a child server. A caching problem can result in advertisements for individual software updates being removed from the policy. This in turn means that the replicated policy is incomplete when it reaches the child and cannot be distributed. The policy needs to be re-created on the parent and replicated again to the child; it cannot be fixed on the child. Symantec recommends that you use the standard replication schedules rather than custom schedules for software update policy replication to avoid this issue.	
A license is not released for retired computers on case-sensitive SQL.	When you retire a computer resource, the Patch Management Solution license is not released. This issue occurs only when case-sensitive SQL Server is used. Workaround: To release the license, delete the resource.	

Table 1-5 Fixed issues *(continued)*

Issue	Description	Article link
Sometimes a software update policy fails to save.	This issue may occur when anonymous access is enabled for the Altiris folder in IIS.	
Package server settings are not migrated from 7.0.	Package server settings on the **Policy and Package Settings** tab are not migrated from 7.0. Configure the settings after the migration.	
Uninstalling the Symantec Management Agent does not remove the Software Update Plug-in.	If you uninstall the Symantec Management Agent from an endpoint, the registry entries that are related to the Software Update Plug-in are not removed. Symantec recommends that before you uninstall the Agent, you uninstall the Software Update Plug-in using the **Software Update Plug-in Uninstall** policy. If the Symantec Management Agent is already uninstalled, use the Windows Installer Clean Up utility to remove the registry entries.	
In certain cases data is not removed for excluded software releases.	If you exclude a software release that was migrated from the 7.x version of the product, its data is not removed from the Inv_Software_Update table and packages are not deleted from C:\Program Files\Altiris\Patch Management\Packages\Updates. You can ignore this issue or clean up the data manually.	

Other things to know

The following are things to know about this release. If additional information about an issue is available, the issue has a corresponding Article link.

Table 1-6 Other things to know

Issue	Description	Article link
You can use the First Time Setup portal to configure Patch Management Solution for the first time.	If you want, you can use the wizard on the **Home > Notification Server Management > First Time Setup** page to configure Patch Management Solution for the first use. Perform the following steps in order: 1 On the portal page, under **Step 5 - Schedule Patch Management**, click **Schedule Patch**. 2 In the wizard, configure the schedules for the patch metadata import tasks. If you want to enable more than one task, make sure the schedules are staggered to prevent the server from overloading. When you turn on the Linux tasks, you must type the Novell Mirror Credentials and the Red Hat Network access credentials. By default, all vendors and all channels are enabled. You can customize the settings later on the appropriate Import Patch Data pages. 3 (Optional) Configure the notification options. If you enable administrator notifications, you must also configure the SMTP Server Settings. You can configure SMTP settings on the **Settings > Notification Server > Notification Server Settings** page. 4 On the next page, configure the assessment scan and update installation schedules or leave the default ones. 5 Click **Schedule patch**.	
The **Download QChain** task is removed from the product.	The QChain software is no longer required to install software updates.	
When a maintenance window is configured, the update installation does not run on the schedule.	If a maintenance window opens before the software update installation schedule, the schedule (including the **Start/End dates**) is disregarded and the software update gets installed before the scheduled time. This issue occurs when **Override Maintenance Windows settings** is not checked. This behavior is expected.	
Close the **Altiris Log Viewer** to improve the performance of the Microsoft and Adobe patch data import tasks.	If you close the **Altiris Log Viewer** when you run the **Import Patch Data for Windows** task, you can improve the task's performance by as much as 50 percent.	

Table 1-6 Other things to know *(continued)*

Issue	Description	Article link
A log file is created on the endpoint.	A log file is created on the endpoint that lets you troubleshoot patch installation issues for the particular computer. The log file location is as follows: `%ALTIRIS_AGENT_INSTALL_FOLDER%\Agents\PatchMgmtAgent\`	
Integrating Patch Management Solution with IT Analytics solution.	IT Analytics solution provides reports that display patch management data. By default, users with **Patch Administrator** role do not have access to these reports. To grant access, add the **IT Analytics Users** role to the users. For more information, see the IT Analytics documentation.	

Documentation that is installed

Table 1-7 Documentation that is included into the product installation

Document	Description	Location
Help	Information about how to use this product. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ The F1 key when the page is active. ■ The **Context** command, which is available in the Symantec Management Console on the **Help** menu.
User Guide	Information about how to use this product. This information is available in PDF format.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. The Documentation Library provides a link to the PDF User Guide on the Symantec support Web site. ■ Supported Products page

Table 1-7 Documentation that is included into the product installation *(continued)*

Document	Description	Location
Symantec Management Platform Help	Information about how to use the Symantec Management Platform	Same as above.

Other information

Table 1-8 Information resources that you can use to get more information

Document	Description	Location
ITMS 7.1 Implementation Guide	Information about capacity recommendations, design models, scenarios, test results, and optimization best practices to consider when planning or customizing ITMS.	http://www.symantec.com/docs/DOC3464
Symantec Management Platform User Guide	Information about using the Symantec Management Platform.	Symantec Management Platform Documentation page
Symantec Management Platform Release Notes	Information about new features and important issues in the Symantec Management Platform.	Symantec Management Platform Documentation page
Symantec Management Platform Installation Guide	Information about using Symantec Installation Manager to install the Symantec Management Platform products.	http://go.symantec.com/sim_doc
Knowledge base	Articles, incidents, and issues about this product.	SymWISE support page
Symantec Connect	An online magazine that contains best practices, tips, tricks, and articles for users of this product.	Symantec Connect page